(19)日本国特許庁（ＪＰ）　(12)公開特許公報(A)　(11)特許出願公開番号
特開2003－87458
(P2003－87458A)
(43)公開日　平成15年３月20日(2003.3.20)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ　1/00		Ｈ０４Ｎ　1/00	Ｃ	２Ｃ０６１
	１０７		１０７Ｚ	５Ｂ０２１
Ｂ４１Ｊ　29/00		Ｇ０６Ｆ　3/12	Ｋ	５Ｃ０６２
Ｇ０６Ｆ　3/12		Ｂ４１Ｊ　29/00	Ｚ	

審査請求　未請求　請求項の数４　ＯＬ　（全 14 頁）

(21)出願番号　特願2001－281218(P2001－281218)

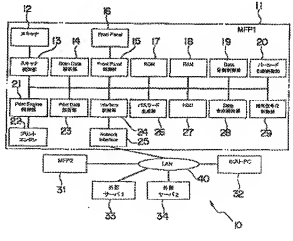
(22)出願日　平成13年９月17日(2001.9.17)

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号
(72)発明者　田中　友輝
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内
(74)代理人　110000062
特許業務法人第一国際特許事務所

Ｆターム(参考)　2C061 AP01 AP07 CL08 CL10
5B021 AA01 NN18
5C062 AA05 AA06 AA35 AB06 AB22
AB42 AC24 AE07 AF12 BA00

(54)【発明の名称】　機密保護機能付き画像形成システム

(57)【要約】
【課題】　印刷データの機密保護をより高めた機密保護機能付き画像形成システムの提供。
【解決手段】　機密保護機能付き画像形成システム１０は、スキャナ１２と、プリントデータ解析部２３と、ＨＤＤ２７と、ネットワークインタフェース２５と、インタフェース制御部２４と、バーコード印刷制御部２０と、スキャンデータ解析部１４を有する。インタフェース制御部２４とネットワークインタフェース２５を用いて情報を外部ファイルサーバ３３，３４或いはＨＤＤ２７に格納する。スキャンデータ解析部１４により得たデータから外部ファイルサーバ３３，３４或いはＨＤＤ２７中の印刷データを読み出して実際のジョブの印刷を行う。



【特許請求の範囲】
【請求項１】　画像読み取り機能を備えた画像形成システムにおいて、
画像の読み取りを行う画像読み取り手段と、受信データから印刷ジョブの機密保護要求を判断する機密保護要求判断手段と、印刷データを記憶する記憶手段と、ネットワークへの接続可能とするネットワークインタフェース手段と、上記ネットワークインタフェース手段を介して外部ファイルサーバ或いは上記記憶手段に情報を格納する印刷データ格納手段と、上記外部ファイルサーバ或いは上記記憶手段に格納された各ジョブのデータが存在する場所を識別情報として印刷する識別情報イメージ生成手段と、上記識別情報イメージ生成手段によって生成された印刷物を読み取りその内容を解析する識別情報イメージ解析手段とを有し、上記機密保護要求判断手段により機密保護要求がなされていると判断した場合に、上記印刷データ格納手段と上記ネットワークインタフェース手段を用いて印刷に必要な情報を全て上記外部ファイルサーバ或いは上記記憶手段に格納し、上記外部ファイルサーバ或いは上記記憶手段のネットワークアドレスも含めて、格納場所を示す識別情報のプリントアウトを上記識別情報イメージ生成手段により作成し、上記識別情報のプリントアウトを上記画像読み取り手段により読み取り、上記識別情報イメージ解析手段により解析し、上記識別情報イメージ解析手段によって得たデータから上記外部ファイルサーバ或いは上記記憶手段中の印刷データを読み出して実際のジョブの印刷を行うことを特徴とする機密保護機能付き画像形成システム。
【請求項２】　上記実際のジョブの印刷に必要な情報を複数に分割するデータ分割手段と、分割された情報を再構成するデータ再構成手段とを有し、上記データ分割手段により分割されたデータを複数の外部ファイルサーバ或いは上記記憶手段からランダムに選択された１つの外部ファイルサーバ或いは記憶手段にそれぞれ格納し、その格納場所及びデータの順序或いは位置情報を識別情報化して印刷し、上記識別情報のプリントアウトを読み込むことによって分割されたデータのそれぞれを順次読み出して再構成し、元データの印刷を可能とした請求項１に記載の機密保護機能付き画像形成システム。
【請求項３】　パスワードを自動的に生成するパスワード自動生成手段と、印刷する識別情報シートに対して識別情報シート番号を付与する識別情報シート番号付与手段と、上記パスワード自動生成手段により生成されたパスワードと識別情報シート番号を機密保護要求が施されたジョブを発行したホストＰＣに通知するパスワード通知手段と、パスワードを入力するパスワード入力手段とを有し、上記識別情報シート印刷時に上記識別情報シート番号付与手段によって識別情報シート番号を付与すると共に、上記パスワード通知手段によってジョブ発行元の上記ホストＰＣに識別情報シート番号と上記パスワード自動生成手段によって生成されたパスワードを通知し、実際のジョブの印刷時に上記パスワード入力手段によるパスワードの入力を要求するようにした請求項１に記載の機密保護機能付き画像形成システム。
【請求項４】　データの暗号化手段と復号化手段を有し、機密保護要求されたジョブの格納時には、パスワード自動生成手段により生成されたパスワードをキーとして、識別情報生成用データ及び実際のジョブの印刷データに上記暗号化手段により暗号化を行い、機密保護要求されて格納されたデータの印刷時には、パスワード入力手段により入力されたパスワードをキーとして識別情報生成用データ及び実際のジョブの印刷データの復号化を行うようにした請求項３に記載の機密保護機能付き画像形成システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、機密保護機能付き画像形成システムに関し、特に、印刷データの機密保護をより高めることと、ネットワーク上に接続された同様の機能を備えた任意の機器から機密保護された情報を取り出すことを可能にすることを主目的としたものである。
【０００２】
【従来の技術】近年、画像形成装置のＭｕｌｔｉ－Ｆｕｎｏｔｉｏｎ化が進み、複写機能と、プリンタ機能と、スキャン機能と、ファクシミリ機能が１台で実現されてきており、さらに、ネットワークへの接続が進んでいるが、印刷データはＭＦＰ（Ｍｕｌｔｉ　Ｆｕｎｏｔｉｏｎ　Ｐｒｉｎｔ）機器内で一旦格納された後に印刷されるため、いつ出力されるのかが不明である。さらに、ネットワーク等から送られる印刷データは、印刷要求者が離れていることが多く、機密文書を印刷した場合には、印刷結果を他人に見られることなく入手するために、ＭＦＰ機器の前で自分の印刷が始まってから完了するまで待ち続ける必要があった。
【０００３】このような問題点を解決するものとして、特開平９－２５１３５８号公報に開示されたように、プリントアウトデータに識別コードを付加し、ユーザーがプリンタ部に同一識別コードを入力した時にのみプリントアウトを可能とする第１の方法や、ユーザーがプリンタ部に識別コードを入力する代わりに識別コードを書き込んだ磁気カードをリーダ部に読み取らせ、その識別コードがプリントアウトデータに含まれる識別コードと一致した時にのみプリントアウトを可能とする第２の方法もあった。
【０００４】さらに、特開平１１－３３４１５８号公報に開示されたように、ユーザー識別コードを記載した力ードを各ユーザーに携帯させ、これを画像読み取り手段にて読み取らせ、このカードに記載されているユーザー識別コードがプリントアウトデータに含まれる識別コー

ドと一致した時にのみプリントアウトを可能とする第３の方法もあった。

【０００５】

【発明が解決しようとする課題】しかしながら、上記特開平９－２５１３５８号公報及び特開平１１－３３４１５８号公報に開示された方法では、いずれも最終的に印刷される印刷データの格納先が当該機器内のメモリであることは明らかであり、当該機器内のメモリをアクセスすることにより、機密性は脆弱なものとなる。また、印刷物を任意の場所から取得することができず、不便であった。

【０００６】本発明は、上記従来の問題点に鑑み、印刷データの格納先を他人に漏らすことなく、安全に格納でき、任意のタイミングで任意の場所からプリントアウトを得ることができ、印刷ジョブの機密保護性を向上させ、さらに、ネットワーク上に接続された周様の機能を持つ任意の機械からでも実際のジョブの印刷を可能とした機密保護機能付き画像形成システムを提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明の機密保護機能付き画像形成システムは、画像読み取り機能を備えた画像形成システムにおいて、画像の読み取りを行う画像読み取り手段と、受信データから印刷ジョブの機密保護要求を判断する機密保護要求判断手段と、印刷データを記憶する記憶手段と、ネットワークへの接続可能とするネットワークインタフェース手段と、上記ネットワークインタフェース手段を介して外部のファイルサーバ或いは上記記憶手段に情報を格納する印刷データ格納手段と、上記外部のファイルサーバ或いは上記記憶手段に格納された各ジョブのデータが存在する場所を識別情報として印刷する識別情報イメージ生成手段と、上記識別情報イメージ生成手段によって生成された印刷物を読み取りその内容を解析する識別情報イメージ解析手段とを有し、上記機密保護要求判断手段により機密保護要求がなされていると判断した場合に、上記印刷データ格納手段と上記ネットワークインタフェース手段を用いて印刷に必要な情報を全て上記外部のファイルサーバ或いは上記記憶手段に格納し、上記外部のファイルサーバ或いは上記記憶手段のネットワークアドレスも含めて、格納場所を示す識別情報のプリントアウトを上記識別情報イメージ生成手段により作成し、上記識別情報のプリントアウトを上記画像読み取り手段により読み取り、上記識別情報イメージ解析手段により解析し、上記識別情報イメージ解析手段によって得たデータから上記外部のファイルサーバ或いは上記記憶手段中の印刷データを読み出して実際のジョブの印刷を行うことを特徴とするものである。

【０００８】本発明の機密保護機能付き画像形成システムは、上記実際のジョブの印刷に必要な情報を複数に分割するデータ分割手段と、分割された情報を再構成するデータ再構成手段とを有し、上記データ分割手段により分割されたデータを複数の外部ファイルサーバ或いは上記記憶手段からランダムに選択された１つの外部ファイルサーバ或いは記憶手段にそれぞれ格納し、その格納場所及びデータの順序或いは位置情報を識別情報化して印刷し、上記識別情報のプリントアウトを読み込むことによって分割されたデータのそれぞれを順次読み出して再構成し、元データの印刷を可能としたものである。

【０００９】本発明の機密保護機能付き画像形成システムは、パスワードを自動的に生成するパスワード自動生成手段と、印刷する識別情報シートに対して識別情報シート番号を付与する識別情報シート番号付与手段と、上記パスワード自動生成手段により生成されたパスワードと識別情報シート番号を機密保護要求が施されたジョブを発行したホストＰＣに通知するパスワード通知手段と、パスワードを入力するパスワード入力手段とを有し、上記識別情報シート印刷時に上記識別情報シート番号付与手段によって識別情報シート番号を付与すると共に、上記パスワード通知手段によってジョブ発行元の上記ホストＰＣに識別情報シート番号と上記パスワード自動生成手段によって生成されたパスワードを通知し、実際のジョブの印刷時に上記パスワード入力手段によるパスワードの入力を要求するようにしたものである。

【００１０】本発明の機密保護機能付き画像形成システムは、データの暗号化手段と復号化手段を有し、機密保護要求されたジョブの格納時には、パスワード自動生成手段により生成されたパスワードをキーとして、識別情報生成用データ及び実際のジョブの印刷データに上記暗号化手段により暗号化を行い、機密保護要求されて格納されたデータの印刷時には、パスワード入力手段により入力されたパスワードをキーとして識別情報生成用データ及び実際のジョブの印刷データの復号化を行うようにしたものである。

【００１１】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて詳細に説明する。図１は本発明の実施の形態における機密保護機能付き画像形成システムを示すブロック図である。本発明の機密保護機能付き画像形成システム１０は、図１に示すように、ＭＦＰ（Ｍｕｌｔｉ Ｆｕｎｃｔｉｏｎ Ｐｒｉｎｔ）機器１１が画像の読み取りを行う画像読み取り手段となるスキャナ１２と、受信データから印刷ジョブの機密保護要求を判断する機密保護要求判断手段となるプリントデータ解析部２３と、印刷データを記憶する記憶手段となるハードディスクドライブ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ；ＨＤＤ）２７と、ローカルエリアネットワーク（ＬｏｃａｌＡｒｅａ Ｎｅｔｗｏｒｋ：ＬＡＮ）４０への接続可能とするネットワークインタフェース手段となるネットワークインタフェース２５と、ネットワークインタフェース２５を介して外部ファイルサーバ３３，３４或いはハードデ

ィスクドライブ（以下ＨＤＤという）２７に情報を格納する印刷データ格納手段となるインタフェース制御部２４と、外部ファイルサーバ３３，３４或いはＨＤＤ２７に格納された各ジョブのデータが存在する場所を識別情報として印刷する識別情報イメージ生成手段となるバーコード印刷制御部２０と、バーコード印刷制御部２０によって生成された印刷物となる識別情報シートを読み取りその内容を解析する識別情報イメージ解析手段となるスキャンデータ解析部１４とを有し、プリントデータ解析部２３により機密保護要求がなされていると判断した場合に、インタフェース制御部２４とネットワークインタフェース２５を用いて印刷に必要な情報を全て外部ファイルサーバ３３，３４或いはＨＤＤ２７に格納し、外部ファイルサーバ３３，３４或いはＨＤＤ２７のネットワークアドレスも含めて、格納場所を示す識別情報のプリントアウトをバーコード印刷制御部２０により作成し、識別情報のプリントアウトをスキャナ１２により読み取り、スキャンデータ解析部１４により解析し、スキャンデータ解析部１４によって得たデータから外部ファイルサーバ３３，３４或いはＨＤＤ２７中の印刷データを読み出して実際のジョブの印刷を行うようになっている。

【００１２】本発明の機密保護機能付き画像形成システム１０は、図１に示すように、ＭＦＰ機器１１が実際のジョブの印刷に必要な情報を複数に分割するデータ分割手段となるデータ分割制御部１９と、分割された情報を再構成するデータ再構成手段となるデータ合成制御部２８とを有し、データ分割制御部１９により分割されたデータを複数の外部ファイルサーバ３３，３４或いはＨＤＤ２７からランダムに選択された１つの外部ファイルサーバ３３，３４或いはＨＤＤ２７にそれぞれ格納し、その格納場所及びデータの順序或いは位置情報を識別情報化して印刷し、識別情報のプリントアウトを読み込むことによって分割されたデータのそれぞれを順次読み出して再構成し、元データの印刷を可能としてある。

【００１３】本発明の機密保護機能付き画像形成システム１０は、図１に示すように、パスワードを自動的に生成するパスワード自動生成手段となるパスワード生成部２６と、印刷する識別情報シートであるバーコードシートに対して識別情報シート番号を付与する識別情報シート番号付与手段となるプリントエンジン２２と、パスワード生成部２６により生成されたパスワードと識別情報シート番号を機密保護要求が施されたジョブを発行したホストＰＣ３２に通知するパスワード通知手段となるフロントパネル制御部１５と、パスワードを入力するパスワード入力手段となるフロントパネル１６とを有し、上記識別情報シート印刷時にプリントエンジン２２によって識別情報シート番号を付与すると共に、フロントパネル制御部１５によってジョブ発行元のホストＰＣ３２に識別情報シート番号とパスワード生成部２６によって生成されたパスワードを通知し、実際のジョブの印刷時にフロントパネル１６によるパスワードの入力を要求するようになっている。

【００１４】本発明の機密保護機能付き画像形成システム１０は、図１に示すように、ＭＦＰ機器１１がデータの暗号化手段と復号化手段となる暗号復号化制御部２９を有し、機密保護要求されたジョブの格納時には、パスワード生成部２６により生成されたパスワードをキーとして、識別情報生成用データ及び実際のジョブの印刷データに暗号復号化制御部２９により暗号化を行い、機密保護要求されて格納されたデータの印刷時には、フロントパネル１６により入力されたパスワードをキーとして識別情報生成用データ及び実際のジョブの印刷データの復号化を行うようになっている。

【００１５】本発明の機密保護機能付き画像形成システム１０は、図１に示すように、ＭＦＰ機器１１とＭＦＰ機器３１とホストＰＣ３２と外部ファイルサーバ３３と外部ファイルサーバ３４とがローカルエリアネットワーク（以下ＬＡＮという）４０を介して接続され、ＭＦＰ機器１１はスキャナ１２と、スキャナ制御部１３と、スキャンデータ解析部１４と、フロントパネル制御部１５と、フロントパネル１６と、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）１７と、ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）１８と、データ分割制御部１９と、バーコード印刷制御部２０と、プリントエンジン制御部２１と、プリントエンジン２２と、プリントデータ解析部２３と、インタフェース制御部２４と、ネットワークインタフェース２５と、パスワード生成部２６と、ＨＤＤ２７と、データ合成制御部２８と、暗号復号化制御部２９を有している。

【００１６】１１は本発明の機密保護機能付き画像形成システム１０の中心となるＭＦＰ機器であり、ＭＦＰ機器１１はスキャナ１２、スキャナ制御部１３、スキャンデータ解析部１４、フロントパネル制御部１５、フロントパネル１６、ＲＯＭ１７、ＲＡＭ１８、データ分割制御部１９、バーコード印刷制御部２０、プリントエンジン制御部２１、プリントエンジン２２、プリントデータ解析部２３、インタフェース制御部２４、ネットワークインタフェース２５、パスワード生成部２６、ＨＤＤ２７、データ合成制御部２８、暗号復号化制御部２９の要素を有する。

【００１７】１２はＭＦＰ機器１１のうち画像の読み取りを行うスキャナである。

【００１８】１３はスキャナ１２の制御を行うスキャナ制御部である。

【００１９】１４はバーコードのデータ解析及び入力画像におけるチェックボックスのチェックの有無の判断を行うスキャンデータ解析部であり、スキャナ１２がスキャナ制御部１３により制御されて読み取った画像データを解析する部分である。

【００２０】１５はフロントパネル１６の制御を行うフロントパネル制御部である。

【００２１】１６はＭＦＰ機器１１のユーザーインタフェースを担うフロントパネルである。

【００２２】１７はＭＦＰ機器１１の全体の制御を行うプログラム及びバーコードフォントを含むフォントデータを格納するためのＲＯＭである。

【００２３】１８はＭＦＰ機器１１の動作中の中間データやイメージデータ用のエリア及びワークエリアとして用いられるＲＡＭである。

【００２４】１９はＲＡＭ１８上に展開されたイメージデータを分割処理するデータ分割制御部であり、イメージデータの分割制御をつかさどる部分である。このデータ分割制御部１９は、自ら分割制御したイメージデータを、インタフェース制御部２４により制御されるネットワークインタフェース２５を介して接続された他のＭＦＰ機器３１を含む外部ファイルサーバ３３，３４に格納する処理を行う。

【００２５】該格納場所に関する情報はＲＡＭ１８上に各々記憶され、これをパスワード生成部２６によって生成されるパスワードをキーとして暗号復号化制御部２９にて暗号化され、当該暗号化されたデータはバーコード印刷制御部２０にてバーコードイメージデータに変換され、ＲＡＭ１８上に展開される。この展開されたデータは、プリントエンジン制御部２１によってプリントエンジン２２に送信され、プリントエンジン２２により印刷される。

【００２６】２０はバーコード印刷制御部であり、ＲＡＭ１８上に記憶されているデータをＲＯＭ１７内に格納されているバーコードフォントデータを用いてバーコードイメージデータとしてＲＡＭ１８上に展開する部分である。該バーコードイメージデータはプリントエンジン制御部２１を介してプリントエンジン２２にて印刷処理される。

【００２７】２１はプリントエンジン２２の制御を行うプリントエンジン制御部であり、実際の印刷の際には、プリントデータ解析部２３，バーコード印刷制御部２０或いはデータ合成制御部２８により作成され、ＲＡＭ１８上にイメージデータとして展開されたデータをプリントエンジン２２に送信することによってプリント処理の制御を行う部分である。

【００２８】２２は実際の印刷処理を行うプリントエンジンである。

【００２９】２３はプリントデータ解析部であり、ＭＦＰ機器１１に対して、インタフェース制御部２４によって制御されるネットワークインタフェース２５を介して、ＬＡＮ４０に接続されたホストＰＣ３２から送信される印刷データを解析し、イメージデータに展開する部分である。このイメージデータに展開する部分において、プリントデータ解析部２３は機密保護要求の判断も行う。

【００３０】２４はインタフェース制御部であり、ネットワークインタフェース２５の制御を行う部分である。このインタフェース制御部２４により、ネットワークインタフェース２５を介して、ＬＡＮ４０に接続されたホストＰＣ３２からの印刷データの受信制御、或いは、同じくＬＡＮ４０に接続された各外部ファイルサーバ３３，３４や他のＭＦＰ機器３１へのデータ送信制御、及び、これらからのデータ取得制御、同じくＬＡＮ４０に接続されたホストＰＣ３２へのパスワード等の情報送信制御を行うようになっている。

【００３１】２５はＭＦＰ機器１１のＬＡＮ４０への接続を可能とするためのネットワークインタフェースである。

【００３２】２６はパスワード生成部であり、プリントデータ解析部２３において機密保持要求がなされていると判断されたジョブを発行したホストＰＣ３２に対して、実際のジョブデータ印刷のためのパスワードを生成する部分である。

【００３３】パスワード生成部２６で生成されたパスワードは、インタフェース制御部２４によって制御されるネットワークインタフェース２５を介して該ジョブを発行したホストＰＣ３２に対してパスワードを通知する。また、このパスワードは、暗号復号化制御部２９においてデータの暗号化を行う時にキーとして用いられる。

【００３４】２７はＨＤＤであり、各ジョブのデータや他のＭＦＰ機器３１から格納要求されたデータを保持するための記憶手段である。このＨＤＤ２７を用いて、このＭＦＰ機器１１はファイルサーバとして動作することも可能となる。

【００３５】２８はイメージデータの合成制御を行うデータ合成制御部であり、上記データ分割制御部１９にて分割処理され、パスワード生成部２６により生成されたパスワードをキーとして暗号復号化制御部２９において暗号化されたデータを元のデータに合成しなおし、ＲＡＭ１８にイメージデータとして展開する制御を行う部分である。

【００３６】この合成に必要な分割されたイメージの格納場所等の情報は、スキャナ１２によって読み取られたバーコードイメージをスキャンデータ解析部１４にて解析処理し、フロントパネル１６から入力されたパスワードをキーとして、暗号復号化制御部２９にて復号化されることによって得られる。復号化することによって得られたこれらの情報が無効な場合、フロントパネル制御部１５を介してフロントパネル１６上にエラーメッセージを表示する。

【００３７】また、ＲＡＭ１８上に展開されたイメージデータは、プリントエンジン制御部２１を介してプリントエンジン２２に送信されて印刷処理される。

【００３８】２９は暗号復号化制御部であり、データ分

割制御部１９において分割されて外部ファイルサーバ３３．３４等に送信されたイメージデータの所在や位置情報等の各種情報及びデータ分割制御部１９にて分割されたイメージデータを、パスワード生成部２６によって生成されたパスワードをキーとした暗号化処理を行い、処理後のデータはバーコード印刷制御部２０に渡される。

【００３９】また、スキャンデータ解析部１４によってバーコード情報から電子情報に変換されたデータ及びこれら情報を用いて外部ファイルサーバ３３，３４や他のＭＦＰ機器３１から取得した暗号化済みのイメージデータの一部を、フロントパネル１６から入力されたパスワード情報をフロントパネル制御部１５から受け取り、これをキーとして復号化処理を行い、処理後のデータはデータ合成制御部２８に渡される。

【００４０】以上までが、本発明の中心となるＭＦＰ機器１１に内蔵されるブロックである。

【００４１】４０はＬＡＮであり、複数の情報機器を接続して任意の機器間でのデータ交換を可能にする。

【００４２】ＬＡＮ４０には、図１に示すように、ＭＦＰ機器１１と、ＭＦＰ機器３１と、文書の作成／編集を行うホストＰＣ３２と、外部ファイルサーバ３３，３４がそれぞれ接続されている。

【００４３】ＭＦＰ機器１１，３１は、それぞれ印刷機器・画像読み取り機器として動作するだけでなく、ファイルサーバとしても動作可能とすることができる。そのため、自分自身も本発明に記述されたファイルサーバとして動作することができる。

【００４４】図２は本発明の機密保護機能付き画像形成システムに係わる受信ジョブ印刷処理の処理フロー図である。まず、印刷ジョブが機密保護機能付き画像形成システム１０のホストＰＣ３２よりＭＦＰ機器１１に送信された時に、ＭＦＰ機器１１のプリントデータ解析部２３において印刷データの解析を行い、機密保護印刷（Ｓｅｃｕｒｅ　Ｐｒｉｎｔ）要求が有るか否かを判断（ステップ１０１）する。

【００４５】ステップ１０１において、機密保護印刷（Ｓｅｃｕｒｅ　Ｐｒｉｎｔ）要求が有ると判断された場合は、機密保護印刷フラグ（Ｓｅｃｕｒｅ　Ｐｒｉｎｔ　Ｆｌａｇ）をＯＮ（ステップ１０２）する。

【００４６】ステップ１０１において、機密保護印刷（Ｓｅｃｕｒｅ　Ｐｒｉｎｔ）要求がないと判断された場合は、ＭＦＰ機器１１のプリントデータ解析部２３において印刷データの解析（ステップ１０３）を続けて行い、次いで、１ページ分のイメージデータの生成（ステップ１０４）を行い、このイメージデータをＭＦＰ機器１１のＲＡＭ１８に展開する。

【００４７】ステップ１０４において、１ページ分のイメージデータの生成が完了した後。機密保護印刷フラグがＯＮされているか否かを判断（ステップ１０５）する。

【００４８】ステップ１０５において、機密保護印刷フラグがＯＮされていると判断された場合は、ＭＦＰ機器１１のパスワード生成部２６においてパスワードの生成（ステップ１０６）を行い、次いで、ステップ１０４においてＭＦＰ機器１１のＲＡＭ１８に展開されたイメージデータを、ＭＦＰ機器１１のデータ分割制御部１９においてイメージデータの分割処理（ステップ１０７）を行う。

【００４９】さらに、ステップ１０７にて得られた分割済みのイメージデータを、ＭＦＰ機器１１の暗号復号化制御部２９において、ステップ１０６にて得られたパスワードをキーとした暗号化処理を行い、処理済のデータをＬＡＮ４０を介してＭＦＰ機器１１に接続された他のＭＦＰ機器３１や外部ファイルサーバ３３，３４にファイルとして送信して保持（ステップ１０８）させる。

【００５０】この時、ステップ１０７にて分割したイメージデータの位置情報やページ情報、及び、ステップ１０８にて送信した送信先のサーバアドレスやファイル名等の情報を、ＭＦＰ機器１１のＲＡＭ１８に保持蓄積する。

【００５１】ステップ１０５において、機密保護印刷フラグがＯＦＦされていると判断された場合には、このページの通常印刷処理（ステップ１０９）を行い、次いで、通常印刷処理がジョブエンドであるか否かを判断（ステップ１１０）する。

【００５２】ステップ１１０において、通常印刷処理がジョブエンドでない場合は、ステップ１０３に戻り、上記ページの通常印刷処理をジョブエンドまで実行する。

【００５３】ステップ１１０において、通常印刷処理がジョブエンドである場合は、再度機密保護印刷フラグがＯＮされているか否かを判断（ステップ１１１）する。

【００５４】ステップ１１１において、機密保護印刷フラグがＯＮされていると判断された場合には、ステップ１０８において保持蓄積した各種情報を、ステップ１０６にて得られたパスワードをキーとして、ＭＦＰ機器１１の暗号復号化制御部２９において暗号化し、この暗号化された情報をＭＦＰ機器１１のＲＯＭ１７に格納されたバーコードフォントデータを用いて、ＭＦＰ機器１１のバーコード印刷制御部２０にてバーコードイメージデータを生成（ステップ１１２）する。

【００５５】次いで、ステップ１１２において生成されたバーコードイメージデータを、ＭＦＰ機器１１のプリントエンジン制御部２１を介してＭＦＰ機器１１のプリントエンジン２２に転送し、バーコードイメージデータの印刷処理（ステップ１１３）を行う。

【００５６】次いで、ステップ１０６にて得られたパスワードを、ＬＡＮ４０を介してこのＭＦＰ機器１１と接続され、現在処理を行っているジョブの発行元であるホストＰＣ３２に対して送信（ステップ１１４）し、パスワードとステップ１１３において印刷されたバーコード

シートに記載されるバーコードシート番号をユーザーに通知し、次いで、機密保護印刷フラグをＯＦＦ（ステップ１１５）にし、その後、現在のジョブを完了し、次のジョブに備える。

【００５７】ステップ１１１において、機密保護印刷フラグがＯＦＦされていると判断された場合には、何も行わずに現在のジョブを完了し、次のジョブに備える。以上が、図２の受信ジョブ印刷処理の処理フローの流れである。

【００５８】図３は図１のＭＦＰ機器１１に機密保持要求がなされた時に印刷されるバーコードシートの一例を示す図である。このバーコードシート５０には、図３に示すように、タイトル５１と、バーコードシート番号５２と、バーコード５３と、印刷後にデータを保存しておくか否かを指示するチェックボックス５４と、印刷せずに保存されたデータを削除するか否かを指示するチェックボックス５５が印刷されている。

【００５９】特に、バーコードシート５０に印刷されたバーコード５３の部分には、このジョブに対する出力者ＩＤやジョブＩＤ等のジョブ情報、各ページに対する用紙サイズや両面指示等の情報を含むページ情報、各ページにおいて分割された部品の位置情報とイメージデータの格納先情報が記述されている。

【００６０】なお、このバーコードシートの一例においては、理解しやすいように各情報ブロック毎に改行処理が施されているが、実際にはその必要はない。

【００６１】図４は図１のＭＦＰ機器１１において、画像読み取り要求がなされた時のスキャンジョブ処理の処理フロー図である。まず、ユーザーが画像読み取りを指示した時、機密保護ジョブ印刷用のバーコード読み取りモードであるか否かを判断（ステップ２０１）し、ステップ２０１において、機密保護ジョブ印刷用のバーコード読み取りモードであると判断した場合には、ＭＦＰ機器１１のフロントパネル制御部１５を介して、ＭＦＰ機器１１のフロントパネル１６にパスワードの入力の要求を促すメッセージを表示（ステップ２０２）し、ユーザーによるパスワードの入力を待つ。

【００６２】次いで、パスワードが入力されると、ＭＦＰ機器１１のスキャナ１２において読み込んだイメージデータをＭＦＰ機器１１のスキャナ制御部１３から受け取り、ＭＦＰ機器１１のスキャンデータ解析部１４においてバーコードデータの解析（ステップ２０３）を行い、次いで、バーコードデータの解析にエラーがあるか否かを判断（ステップ２０４）する。

【００６３】ステップ２０４において、このバーコードデータの解析にエラーがあったと判断された場合には、読み込んだイメージデータが機密保護ジョブの再構成用バーコードイメージではないと判断し、ＭＦＰ機器１１のフロントパネル制御部１５を介してＭＦＰ機器１１のフロントパネル１６にその旨を示すエラーメッセージを表示（ステップ２０９）し、その後、ジョブを終了する。

【００６４】ステップ２０４において、バーコードデータの解析にエラーがないと判断された場合には、ＭＦＰ機器１１の暗号複号化制御部２９において、解析後のバーコードデータをステップ２０２において得たパスワードをキーとして復号化処理（ステップ２０５）を行い、次いで、復号化された情報から印刷要求されている機密保護ジョブにおいて分割／暗号化／保存された全てのデータの存在を検証（ステップ２０６）し、次いで、全データが存在するか否かを判断（ステップ２０７）する。

【００６５】ステップ２０７において、全データの存在が確認された場合には、元イメージデータの復元処理（ステップ２０８）を行った後、このジョブを終了する。

【００６６】ステップ２０７において、一部のデータが欠損していると判断した場合には、外部接続されている外部ファイルサーバ３３，３４に問題があると判断し、ＭＦＰ機器１１のフロントパネル制御部１５を介してＭＦＰ機器１１のフロントパネル１６にその旨を示すエラーメッセージを表示（ステップ２０９）し、その後、ジョブを終了する。

【００６７】ステップ２０７において、全てのデータが存在しない場合には、ステップ２０２において入力されたパスワードが不正なものであると判断し、ＭＦＰ機器１１のフロントパネル制御部１５を介してＭＦＰ機器１１のフロントパネル１６にその旨を示すエラーメッセージを表示（ステップ２０９）し、その後、ジョブを終了する。

【００６８】ステップ２０１において、機密保護ジョブ印刷用のバーコード読み取りモードでないと判断した場合には、通常の画像読み取り処理であるスキャン処理（ステップ２１０）を行い、その後、ジョブを終了する。

【００６９】図５は図４の元イメージデータの復元処理（ステップ２０８）の詳細な処理フロー図である。まず、ＭＦＰ機器１１のスキャンデータ解析部１４において、読み取られた図３のバーコードシート５０上で、印刷せずに保存されたデータを削除するか否かを指示する図３のチェックボックス５５にユーザーによるチェックが施されているか否かを判断（ステップ３０１）し、ステップ３０１において、バーコードシート５０のチェックボックス５５にユーザーによるデータ削除のチェックが施されていると判断した場合には、図４の全データの存在検証処理（ステップ２０６）において得られた、読み取られたバーコードシート５０に対応する図１の外部ファイルサーバ３３，３４上の全てのデータの削除処理（ステップ３０６）を行い、この処理を抜ける。

【００７０】ステップ３０１において、バーコードシート５０のチェックボックス５５にユーザーによるデータ

削除のチェックが施されていないと判断した場合には、図４のバーコード解析処理（ステップ２０３）、図４のパスワードによる復号化処理（ステップ２０５）、図４の全データの存在検証処理（ステップ２０６）において得られた各種情報から、図１の外部ファイルサーバ３３，３４等に格納されたデータを順次取得（ステップ３０２）し、取得したデータを、図４のステップ２０２にて得られたパスワードをキーとしてＭＦＰ機器１１の暗号復号化制御部２９において復号化を行い、ページ単位でイメージデータの再構成（ステップ３０３）を行う。

【００７１】再構成されたページデータは、ＭＦＰ機器１１のＲＡＭ１８上に展開され、ＭＦＰ機器１１のプリントエンジン制御部２１を介してＭＦＰ機器１１のプリントエンジン２２に転送され、印刷処理される。

【００７２】次いで、ステップ３０３において印刷処理されたページにてジョブが完了しているか否かを判断（ステップ３０４）し、ステップ３０４において、ジョブが完了していると判断した場合には、ＭＦＰ機器１１のスキャンデータ解析部１４において、読み取られた図３のバーコードシート５０上で、印刷後にデータを保存しておくか否かを指示する図３のチェックボックス５４にユーザーによるチェックが施されているか否かを判断（ステップ３０５）し、ステップ３０５において、バーコードシート５０のチェックボックス５４にユーザーによるデータ保存のチェックが施されていないと判断した場合には、図４の全データの存在検証処理（ステップ２０６）において得られた、読み取られたバーコードシート５０に対応する図１の外部ファイルサーバ３３，３４上の全てのデータの削除処理（ステップ３０６）を行い、この処理を抜ける。

【００７３】上記ステップ３０５において、バーコードシート５０のチェックボックス５４にユーザーによるデータ保存のチェックが施されていると判断した場合には、読み取られたバーコードシート５０に対応する外部データの削除処理は行わず、この処理を抜ける。

【００７４】このことによって、同じバーコードシートとパスワードを用いて、ユーザーはこのジョブの再出力を行うことができる。

【００７５】ステップ３０４において、ジョブが完了していないと判断した場合には、ステップ３０２に戻って、次のページの処理を続ける。

【００７６】なお、本発明の実施の形態では、特許請求の範囲にて記述された識別情報としてバーコードを用いているが、特にバーコードに限定するものではなく、例えば数字列や文字列を用いて識別を行うことも可能であることはいうまでもない。

【００７７】

【発明の効果】以上に述べたように、本発明の機密保護機能付き画像形成システムによれば、機密保護要求判断手段により受信データから印刷ジョブの機密保護要求がなされていると判断した場合に、印刷データ格納手段とネットワークインタフェース手段を用いて印刷に必要な情報を全て外部ファイルサーバ或いは記憶手段に格納することができ、外部ファイルサーバ或いは記憶手段のネットワークアドレスも含めて、格納場所を示す識別情報のプリントアウトを識別情報イメージ生成手段により生成することができ、画像読み取り手段が識別情報イメージ生成手段により生成された識別情報のプリントアウトした印刷物を読み取るので、その内容を識別情報イメージ解析手段により解析することができ、識別情報イメージ解析手段により得られたデータから外部ファイルサーバ或いは記憶手段中の印刷データを読み出して実際のジョブの印刷を行え、機密保護された印刷データを印刷するトリガとして、識別情報（例えばバーコード）の印刷物を用いているため、印刷システム単体ではその機密保護要求された印刷データそのものが存在することが漏れることもなく、印刷ジョブのより高い機密保護を行うことができる。また、ネットワークに接続された外部ファイルサーバへもデータの保存が可能であるので、機密保護要求された印刷データの所在も隠蔽することができ、印刷ジョブのより高い機密保護性の向上が図れ、ネットワークに接続された同様の機能を持つ別のマシンからでも、実際のジョブの印刷を行うことが可能である。

【００７８】本発明の機密保護機能付き画像形成システムによれば、機密保護を要求された印刷に対して、データ分割手段が実際のジョブの印刷に必要な情報を複数に分割するので、データ分割手段により分割されたデータを外部ファイルサーバ或いは記憶手段にばらばらに格納することができ、分割された一つ一つのデータは、その全体の部分でしかない。また、分割されたデータを再構成するに際し、その格納場所及びデータの順序或いは位置情報を識別情報化して印刷し、識別情報のプリントアウトを読み込むことにより、データ再構成手段が分割されたデータのそれぞれを原次読み出して再構成するので、元データの印刷を行うことができ、別途出力した識別情報のプリントアウトした印刷物を用いるため、印刷ジョブのより高い機密保護性の向上を図ることができる。

【００７９】本発明の機密保護機能付き画像形成システムによれば、識別情報シート印刷時に、識別情報シートに対して識別情報シート番号付与手段により識別情報シート番号を付与することができ、パスワード自動生成手段がパスワードを自動的に生成するので、ジョブ発行元のホストＰＣにパスワード通知手段により識別情報シート番号とパスワードを通知することができ、実際のジョブの印刷時に、パスワードのパスワード入力手段による入力を要求するようにしたので、識別情報シートそのものを期待しない者に使用された場合にも、実際のジョブの印刷のためには、パスワード入力手段にパスワードを入力しなければならず、印刷ジョブのより高い機密保護

性の向上を図ることができる。

【００８０】本発明の機密保護機能付き画像形成システムによれば、機密保護要求されたジョブの格納時に、パスワード自動生成手段により生成されたパスワードをキーとして、識別情報生成用データ及び実際のジョブの印刷データに暗号化手段により暗号化を行うことができ、識別情報シートを期待しない者により識別情報データが解析された場合にも、識別情報データは暗号化手段により暗号化されているため、パスワードを知らなければ、実際のジョブの印刷データの格納場所の機密を保つことができる。また、この実際のジョブの印刷データは同じく暗号化手段によって暗号化されているため、自分自身を含むファイルサーバ内のファイルを期待しない者が覗いても、意味のあるデータは存在しないため、印刷ジョブのより高い機密保護性の向上を図ることができる。さらに、機密保護要求されて格納されたデータの印刷時に、パスワード入力手段により入力されたパスワードをキーとして、識別情報生成用データ及び実際のジョブの印刷データの復号化を行うことができる。

【図面の簡単な説明】

【図１】本発明の実施の形態における機密保護機能付き画像形成システムを示すブロック図。

【図２】本発明の機密保護機能付き画像形成システムに係わる受信ジョブ印刷処理の処理フローチャート図。

【図３】図１のＭＦＰ機器に機密保持要求がなされた時に印刷されるバーコードシートの一例を示す図。

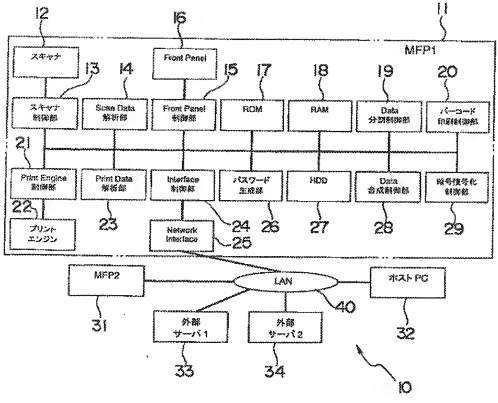
【図４】図１のＭＦＰ機器において画像読み取り要求がなされた時のスキャンジョブ処理の処理フローチャート図。

【図５】図４の元イメージデータの復元処理の詳細な処理フローチャート図。

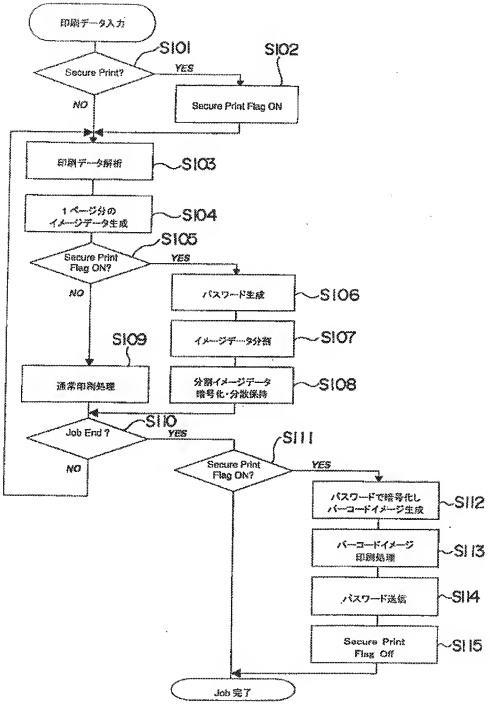
【符号の説明】

１０　機密保護機能付き画像形成システム
１１　ＭＦＰ機器
１２　スキャナ
１３　スキャナ制御部
１４　スキャンデータ解析部
１５　フロントパネル制御部
１６　フロントパネル
１７　ＲＯＭ
１８　ＲＡＭ
１９　データ分割制御部
２０　バーコード印刷制御部
２１　プリントエンジン制御部
２２　プリントエンジン
２３　プリントデータ解析部
２４　インタフェース制御部
２５　ネットワークインタフェース
２６　パスワード生成部
２７　ハードディスクドライブ
２８　データ合成制御部
２９　暗号復号化制御部
３１　ＭＦＰ機器
３２　ホストＰＣ
３３　外部ファイルサーバ
３４　外部ファイルサーバ
４０　ＬＡＮ
５０　バーコードシート
５１　タイトル
５２　バーコードシート番号
５３　バーコード
５４　チェックボックス
５５　チェックボックス

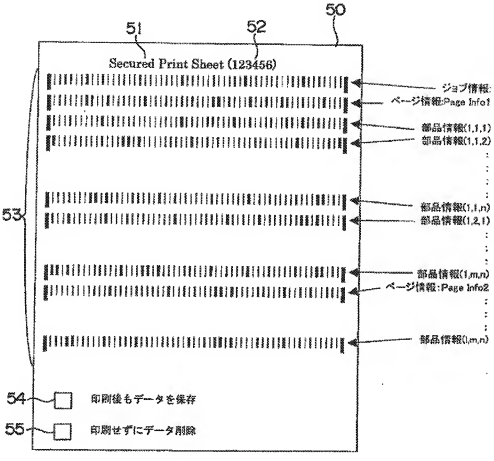
【図１】


12
16
11
MFP1
スキャナ
Front Panel
13
14
15
17
18
19
20
スキャナ制御部
Scan Data解析部
Front Panel制御部
ROM
RAM
Data分割制御部
バーコード印刷制御部
21
Print Engine制御部
Print Data解析部
Interface制御部
パスワード生成部
HDD
Data合成制御部
暗号復号化制御部
22
23
24
25
26
27
28
29
プリントエンジン
Network Interface
MFP2
LAN
ホストPC
40
31
外部サーバ1
外部サーバ2
32
33
34
10

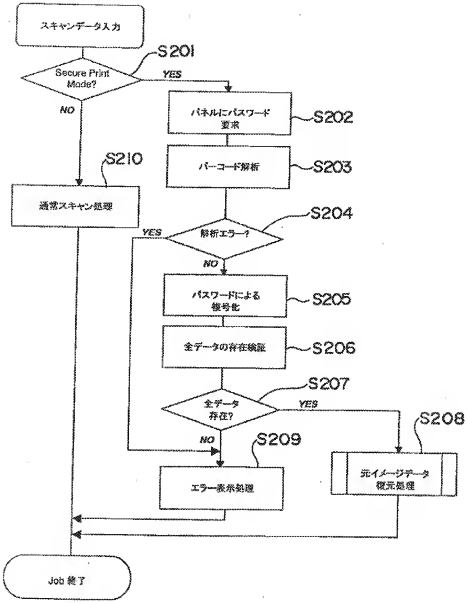
【図２】


印刷データ入力
S101
Secure Print?
YES
S102
Secure Print Flag ON
NO
印刷データ解析
S103
1ページ分の
イメージデータ生成
S104
S105
Secure Print
Flag ON?
YES
NO
パスワード生成
S106
イメージデータ分割
S107
分割イメージデータ
暗号化・分散保持
S108
S109
通常印刷処理
S110
Job End ?
YES
NO
S111
Secure Print
Flag ON?
YES
パスワードで暗号化し
バーコードイメージ生成
S112
バーコードイメージ
印刷処理
S113
パスワード送信
S114
Secure Print
Flag Off
S115
Job 完了

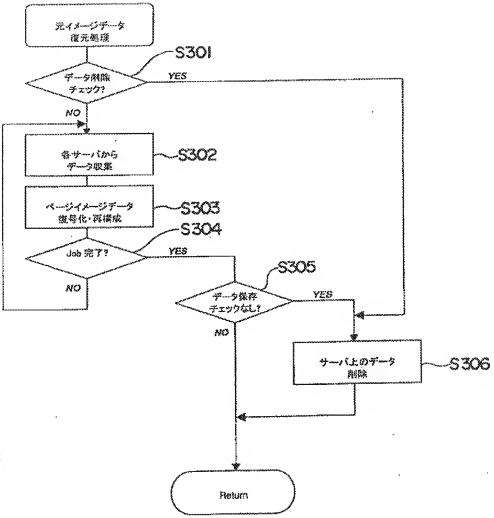
【図３】


50
51
52
Secured Print Sheet (123456)
ジョブ情報:
ページ情報:Page Info1
部品情報(1,1,1)
部品情報(1,1,2)
部品情報(1,1,n)
部品情報(1,2,1)
部品情報(1,m,n)
ページ情報:Page Info2
部品情報(1,m,n)
53
54
印刷後もデータを保存
55
印刷せずにデータ削除

【図４】


スキャンデータ入力
S201
Secure Print Mode?
YES
NO
パネルにパスワード要求
S202
バーコード解析
S203
S210
通常スキャン処理
S204
解析エラー?
YES
NO
パスワードによる復号化
S205
全データの存在検証
S206
S207
全データ存在?
YES
NO
S208
S209
エラー表示処理
元イメージデータ復元処理
Job 終了

【図５】


元イメージデータ
復元処理
S301
データ削除
チェック?
YES
NO
各サーバから
データ収集
S302
ページイメージデータ
復号化・再構成
S303
S304
Job 完了?
YES
NO
S305
データ保存
チェックなし?
YES
NO
サーバ上のデータ
削除
S306
Return

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-087458
(43)Date of publication of application : 20.03.2003

(51)Int.Cl. H04N 1/00
B41J 29/00
G06F 3/12

(21)Application number : 2001-281218
(22)Date of filing : 17.09.2001

(71)Applicant : SHARP CORP
(72)Inventor : TANAKA TOMOKI

(54) IMAGE FORMING SYSTEM WITH SECURITY PROTECTING FUNCTION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an image forming system with a security protecting function that can enhance security protection of print data much more.
SOLUTION: The image forming system 10 with a security protecting function includes a scanner 12, a print data analysis section 23, an HDD 27, a network interface 25, an interface control section 24, a bar code print control section 20, and a scan data analysis section 14. Using the interface control section 24 and the network interface 25 stores information to external file servers 33, 34 or the HDD 27. Print data in the external file servers 33, 34 or the HDD 27 are read on the basis of the data obtained from the scan data analysis section 14 and used for the print of an actual job.